Elektrobit

UDACITY

Technical Safety Concept: Lane Assistance

Document version: 0.1

Template version: 1.0, Released on 2017-06-21

Author:
Konstantin Selyunin

August 27, 2018

Revision History

Version	Date	Editor	Description
0.1	2018/08/23	Konstantin Selyunin	LaTeX template created
0.2	2018/08/26	Konstantin Selyunin	Filling the content part

Contents

1 Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to refine the previously defined functional safety requirements to the hardware and software architecture to take into account technical details, system limitations, and architecture.

According to the ISO 26262 [1] the technical safety concept is part of the product development phase.

The main tasks of technical safety concept include:

- Turning functional safety requirements into technical safety requirements
- Allocating technical safety requirements to the system architecture

2 Inputs to the Technical Safety Concept

2.1 Functional Safety Requirements

The functional safety requirements for the lane assistance item are presented in Table 21

Table 21: Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	the system is turned off
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	the system is turned off
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	The lane keeping functionality is turned off

2.2 Refined System Architecture from Functional Safety Concept

The refined architecture of the lane assistance item is shown in Figure 21.

2.2.1 Functional overview of architecture elements

The functional overview of the architecture elements is shown in Table 22.

Table 22: Architecture elements

Element	Descriptiion
Camera Sensor	provides Image to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	performs image processing and identifies position of a vehicle w.r.t. the lane
Camera Sensor ECU - Torque request generator	Generates a request for EPS ECU to apply steering torque to keep a vehicle on the center of the lane
Car Display	displays the status of the lane assistance item
Car Display ECU - Lane Assistance On/Off Status	displays on a car display whether a lane assistance item is On/Off
Car Display ECU - Lane Assistant Active/Inactive	displays on a car display whether lane assistant is currently active
Car Display ECU - Lane Assistance malfunction warning	informs a driver that a lane assistance item malfunctions
Driver Steering Torque Sensor	senses the position of the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	gets an input steering torque from the driver
EPS ECU - Normal Lane Assistance Functionality	calculates steering torque to keep the vehicle on the center of the road
EPS ECU - Lane Keeping Assistant Safety Functionality	monitors Lane Keeping Assistant for Malfunctions and if a malfunction is detected a signal is sent to the car display to inform the driver and an item is shut down
EPS ECU - Lane Departure Warning Safety Functionality	monitors Lane Departure Warning for Malfunctions and if a malfunction is detected a signal is sent to the car display to inform the driver and an item is shut down
EPS ECU - Final Torque	given current velocity, steering torque from the driver and status of the lane assistance item calculate a final torque applied to steer the car
Motor	activates vibrations of the steering wheel

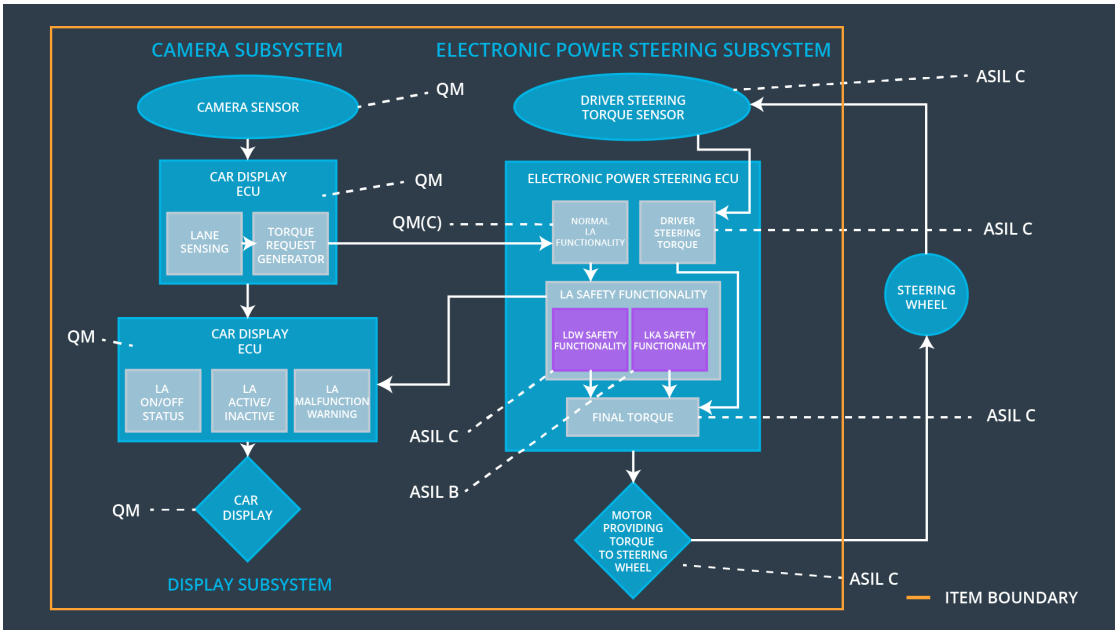

Figure 21: Refined architecture

3 Technical Safety Concept

3.1 Technical Safety Requirements

3.1.1 Lane Departure Warning (LDW) Requirements

Functional Safety Requirement 01-01 with its associated system elements (derived in the functional safety concept) presented in Table 31.

Table 31: Functional Safety Requirement

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	✓		

Technical Safety Requirements related to Functional Safety Requirement 01-01 presented in the Table 32

Functional Safety Requirement 01-02 with its associated system elements (derived in the functional safety concept) is presented in Table 33.

Technical Safety Requirements related to Functional Safety Requirement 01-02 are presented in Table 34.

3.1.2 Lane Keeping Assistance (LKA) Requirements

Functional Safety Requirement 02-01 with its associated system elements (derived in the functional safety concept) is presented in Table 35).

Technical Safety Requirements related to Functional Safety Requirement 02-01 are presented in Table 36.

3.2 Refinement of the System Architecture

The refined architecture after specifying technical safety requirements is shown on Figure 31

Table 32: Technical Safety Requirements for Functional Safety Requirement 01-01

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01-01-01	The LDW safety component shall ensure that the amplitude of the LDW_Torque_Request sent to the **'Final electronic power steering Torque'** component is below Max_Torque_Amplitude	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off
Technical Safety Requirement 01-01-02	As soon as the LDW function deactivates the LDW feature, the **'LDW Safety'** software block shall send a signal to the car display ECU to turn on a warning light	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off
Technical Safety Requirement 01-01-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the LDW_Torque_Request shall be set to zero	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	ignition cycle	**Memory Management Unit**	the lane assistance item is turned off

Table 33: Functional Safety Requirement

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	✓		

Table 34: Technical Safety Requirements for Functional Safety Requirement 01-02

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01-02-01	The LDW safety component shall ensure that the frequency of the LDW_Torque_Request sent to the **'Final electronic power steering Torque'** component is below Max_Torque_Frequency	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off
Technical Safety Requirement 01-02-02	As soon as the LDW function deactivates the LDW feature, the **'LDW Safety'** software block shall send a signal to the car display ECU to turn on a warning light	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off
Technical Safety Requirement 01-02-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the LDW_Torque_Request shall be set to zero	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off
Technical Safety Requirement 01-02-04	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off
Technical Safety Requirement 01-02-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	ignition cycle	**Memory Management Unit**	the lane assistance item is turned off

Table 35: Functional Safety Requirement

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	✓		

Table 36: Technical Safety Requirements for `Functional Safety Requirement 02-01`

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
`Technical Safety Requirement 02-01-01`	The LKA safety component shall ensure that the time interval of applying the `LKA_Torque_Request` is below `Max_Duration`	B	500 ms	**LKA Safety** Software Block	the lane assistance item is turned off
`Technical Safety Requirement 02-01-02`	As soon as the LKA function deactivates the LKA feature, the **'LKA Safety'** software block shall send a signal to the car display ECU to turn on a warning light	B	500 ms	**LKA Safety** Software Block	the lane assistance item is turned off
`Technical Safety Requirement 02-01-03`	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the `LKA_Torque_Request` shall be set to zero	B	500 ms	**LKA Safety** Software Block	the lane assistance item is turned off
`Technical Safety Requirement 02-01-04`	The validity and integrity of the data transmission for `LKA_Torque_Request` signal shall be ensured	B	500 ms	**LKA Safety** Software Block	the lane assistance item is turned off
`Technical Safety Requirement 02-01-05`	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	ignition cycle	**Memory Management Unit**	the lane assistance item is turned off

3.3 Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering ECU.

3.4 Warning and Degradation Concept

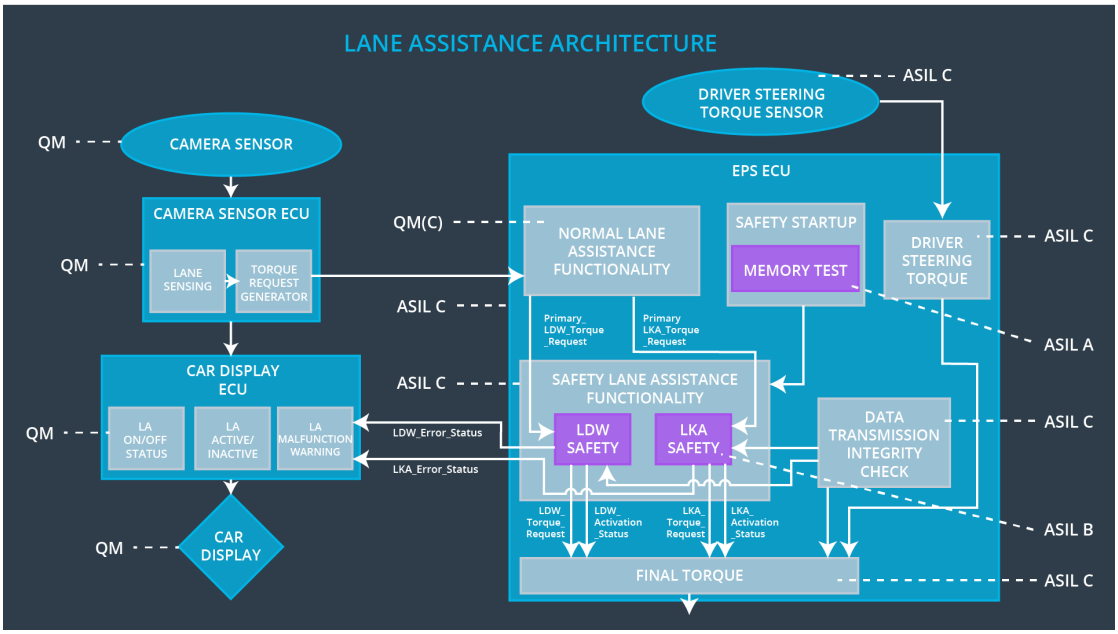

Figure 31: Refined architecture

Table 37: Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the functionality	Malfunction1, Malfunction2	Yes	Indication light on car display on
WDC-02	Turn off the functionality	Malfunction3	Yes	Indication light on car display on

4 List of Abbreviations

ISO	International Organization for Standardization
ASIL	Automotive Safety Integrity Level
ECU	Electronic Control Unit
EPS	Electronic Power Steering
OEM	Original Equipment Manufacturer
LDW	Lane Departure Warning
LKA	Lane Keeping Assistance

Bibliography

[1] Organización Internacional de Normalización. *ISO 26262: Road Vehicles : Functional Safety*. ISO, 2011.